Frequently Asked Questions

Q) What is NSCAP?
A) NSCAP, the National Security Cyber Assistance Program, is an initiative sponsored by the National Security Agency's Information Assurance Directorate to accredit qualified organizations in performing select cybersecurity services in support of national security system (NSS) owners and operators. By capitalizing on the resources, skills, and expertise available, NSCAP aims to narrow the gap between the growing demand for cyber defense services and the U.S. government's ability to meet the demand. As a formal standardized program, NSCAP affirms that accredited organizations have the processes, procedures, resources, and competencies in place to deliver cybersecurity services to NSS owners and operators.

Q) What is a National Security System?
A) *A National Security System (NSS) is any information system (including any telecommunications system) used or operated by an agency, a contractor of an agency, or other organization on behalf of an agency where the use or operation involves intelligence activities, cryptologic activities related to national security, command and control of military forces, or is an integral part of a weapon or weapons system. This definition also encompasses systems used to support military or intelligence missions. Systems that are specifically identified within approved legislation or executive order and must be kept classified in the interest of national defense or foreign policy are also considered to be NSS. All U.S. government classified networks have been designated as NSS.*

Q) What is CIRA?
A) *NSA/IAD is following a phased approach to implement NSCAP, beginning with CIRA, or Cyber Incident Response Assistance, accreditation. NSA/IAD will award CIRA accreditation to firms deemed qualified to provide rapid, on-site support to National Security System owners and operators in incident response and intrusion detection. To qualify, candidate firms must demonstrate competency and expertise, as identified on the NSA.Gov website and within the accreditation instruction manual.*

Q) Who may apply for NSCAP Cyber Incident Response Assistance (CIRA) accreditation?
A) *Any U.S. Organization that offers CIRA services as a core part of its business model.*

Q) What is the accreditation process?
A) The *candidate organization will assemble a complete application package as outlined in Appendix C of the Program Instruction Manual downloadable from NSA.Gov*

Q) **Where can I find a copy of the Program Instruction Manual?**
*A) The **Program Instruction Manual** is available on the NSCAP website and linked here for your convenience.*

Q) **How do I submit my organization's application package?**
A) *Instructions on how and when to submit your organizations Application packages will be posted on the program website and on the ARC website at regularly occurring intervals.*

Q) Is there an application fee?
A) *Candidate organizations* ***are not charged any fee*** *for applying for accreditation. Additionally, the NSA/IAD* ***will not*** *fund any portion of the costs incurred by an applicant/ candidate Organization to work through the accreditation process or, once accredited, to maintain accreditation status.*

Q) If accredited, how will my company be contacted to perform services?
A) *Your company's contact information will be added to the list of accredited companies. When an NSS system owner has an issue that the NSA cannot respond to in a timely manner, that organization will be pointed to the list of accredited service providers.*

Q) How long is the accreditation valid?
A) *It is valid for 24 months*.

Q) What is required for accreditation renewal?
A) *Renewals require the organization to resubmit any documentation modified since the original submission so that it can be reevaluated by NSCAP project evaluators. Organizations must also present two past performance summaries from work performed during the previous accreditation period. Past performance does not have to be in support of NSS.*

Q) Our organization provides incident response assistance services under a Managed Security Services model where services are provided through remote monitoring. Is this model acceptable for earning an accreditation?
A) *CIRA accreditation is for on-site incident response services that include intrusion detection, malware analysis and reverse engineering, forensics, PCAP and network traffic analysis, host integrity checking, containment, eradication, remediation, and on-going mitigations. Additionally, there are expectations that the candidate organization will be fully positioned to provide these services when needed and that the provisioning of these services is not dependent on the client purchasing some other service or product from the candidate. As NSS owners and operators may not be able to move data and information to remote locations for analysis and support, the work needs to be performed on site. This answer also applies to outsourcers that provide incident response assistance services as part of their outsourcing service offering.*

Q) Will the NSA/IAD provide accredited organizations with information to support their service delivery to clients?
A) *The contractual relationship between the CIRA-accredited service provider and client would not normally include the NSA/IAD. Therefore, the NSA/IAD will not transfer information directly to the service provider. If requested by the client, the NSA/IAD may provide information to support the client's incident response activities. To accommodate this possibility, the candidate organization must submit its "property management" plan as part of its application package.*

Q) Does CIRA accreditation cover all information systems used by the federal government?
A) *This program is to accredit firms that have met requirements to address incidents on National Security Systems only, consistent with NSA/IAD's authority.*